Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

The expression

$$\chi = \psi_1 + \omega\psi_2 + \omega^2\psi_3 + \ldots . \omega^{\nu-1}\psi_\nu$$

is then a function of $x_1, x_2, \ldots . x_n$ which belongs* to the group H and satisfies a binomial resolvent equation

$$\chi^\nu = R(\phi; c_1, c_2, \ldots . c_n). \qquad \text{Q. E. D.}\dagger$$

§9.—*Decomposition of Groups, in particular of the Symmetric Group.*

43. Every group has two self-evident self-conjugate subgroups, viz. itself and the group 1; if it contain no other self-conjugate subgroup, it is called a *simple group;* otherwise, a *composite group.*

A composite group G can be *decomposed* in the following way: From the group G we descend to a *maximal self-conjugate subgroup* H; that is, a self-conjugate subgroup of G which is not contained in a larger self-conjugate subgroup of G; from H we descend to a maximal self-conjugate subgroup I of H, and so on until at last we arrive at the group 1. Such a series of groups

$$\begin{array}{cccccc} G, & H, & I \ldots . & M, & 1, \\ \lambda & \mu & & \rho & \end{array}$$

in which each group is a maximal self-conjugate subgroup of the group immediately preceding it, is called a *series of composition* of the group G, and the successive indices λ (index of H under G), μ (index of I under H) $\ldots . \rho$ are called the *factors of composition.*

Examples:‡ (Compare No. 36).

1). Symmetric group of three letters:

$$G_6,\ G_3,\ 1.$$

2). Symmetric group of four letters:

$$G_{24},\ G_{12},\ G_4,\ G_2,\ 1;$$

instead of the group

$$G_2 = [1, (1\,2)(3\,4)],$$

---

* ψ can always be chosen such (viz. by replacing, if necessary, ψ by $\psi\ (m+\psi)$) that χ remains unaltered by *no other* substitutions than those of G (see also Netto, §102).

† References concerning §9: Jordan, No. 67-74; Netto, §87-92; König, l. c. §1; Capelli, l. c. III.

‡ From No. 36 it follows easily that a subgroup of index 2 is always a self-conjugate subgroup.

we may also choose the similar groups

$$G_2' = [1, (1\,3)(2\,4)],$$

or

$$G_2'' = [1, (1\,4)(2\,3)].$$

It may happen that there exist several decompositions of the same group, as in the last example; in this case, however, *the factors of composition for the different decompositions are the same excepting their order.* For the proof of this theorem we refer to Netto, §81.

44. *The series of composition of the symmetric group of n letters consists of the symmetric group, the alternate group and the group* 1:

$$G_{n!},\ G_{\frac{n!}{2}},\ 1, \tag{1}$$

excepting the only case $n = 4$.

Proof: 1). The alternate group is a *self-conjugate* subgroup of the symmetric group, since (No. 36) the transformed of an even substitution by any substitution is always an even substitution; moreover, it is a *maximum* self-conjugate subgroup, since the index $\nu = 2$ is prime.

2). *The alternate group is simple,* excepting the case $n = 4$; the proof is founded on the following principle: If a self-conjugate subgroup H of a group G contain a substitution h, then it contains also all those substitutions which are conjugate with h under G, say

$$h,\ h',\ h'',\ \ldots.\ h^{(\mu-1)}, \tag{2}$$

and therefore also the group generated by these substitutions,

$$G(h,\ h',\ h''\ \ldots.\ h^{(\mu-1)}) \qquad \text{(see No. 19)},$$

which we will denote by H_h.

In the present case G is the alternate group $G_{\frac{n!}{2}}$:

a). Let us first choose for h a circular substitution of three letters, say

$$h = (1\,2\,3),$$

which is sure to be contained in $G_{\frac{n!}{2}}$, since it is an even substitution (No. 16).

The corresponding series (2) *of conjugate substitutions consists of all the circular substitutions of three letters;* that is to say, it is always possible to find in $G_{\frac{n!}{2}}$ a substitution g which transforms $(1\,2\,3)$ into any other circular substitution $(\alpha\beta\gamma)$:

$$(\alpha\beta\gamma) = g^{-1}(1\,2\,3)\,g;$$

namely, one of the two substitutions

$$a = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \ldots\ldots n \\ \alpha\ \beta\ \gamma\ \delta\ \varepsilon \ldots\ldots \lambda \end{pmatrix}$$

and

$$a' = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \ldots\ldots n \\ \alpha\ \beta\ \gamma\ \varepsilon\ \delta \ldots\ldots \lambda \end{pmatrix} = a.(\delta\varepsilon),$$

both of which transform (1 2 3) into $(\alpha\beta\gamma)$ (No. 34), is sure to be even and may therefore be chosen for g.*

b). *The group H_h, generated by all the circular substitutions of three letters, is the alternate group.*

For the product of any two transpositions can always be written as a product of circular substitutions of three letters; namely, if the two transpositions have one letter in common, we have

$$(\alpha\beta)(\alpha\gamma) = (\alpha\beta\gamma),$$

if they have no letter in common, we have

$$(\alpha\beta)(\gamma\delta) = (\alpha\beta)(\alpha\gamma).(\gamma\alpha)(\gamma\delta) = (\alpha\beta\gamma).(\gamma\alpha\delta).$$

Hence any even substitution can be decomposed into a product of circular substitutions of three letters; and since, conversely, the product of any number of circular substitutions of three letters is always even, our statement is proved and we have $H_h = G_{\frac{n!}{2}}$, if h is a circular substitution of three letters.

c). To this case all other cases can be reduced; namely, if we choose for h any other substitution, it is always possible to form out of the conjugate substitutions (2) a product which is a circular substitution of three letters.

We confine ourselves to the case $n = 5$, referring for the general case to Netto, §84.

The alternate group of five letters, G_{60} contains, besides the circular substitutions of three letters, substitutions of the types (1 2)(3 4) and (1 2 3 4 5).

α). If H contain the substitution $h = (1\,2)(3\,4)$, it contains also the transformed of h by the even substitution $g = (1\,2)(4\,5)$, viz. $h' = (2\,1)(3\,5)$, and consequently also the product $hh' = (3\,4\,5)$; hence $H = G_{60}$ according to *b*).

(This conclusion cannot be reached if $n = 4$, which accounts for the existence of the self-conjugate subgroup G_4 of G_{12}.)

---

* This conclusion can be reached only when $n > 4$.

β). If H contain the substitution $h = (1\,2\,3\,4\,5)$, it contains also the transformed of h by the even substitution $g = (2\,3)(4\,5)$, viz. $h' = (1\,3\,2\,5\,4)$ and consequently also the product $hh' = (1\,5\,3)$; hence again $H = G_{60}$.

Thus the alternate group of five letters is indeed found to be simple.

45. The above decomposition (1) of the symmetric group is the only possible one; or, in other words, *the alternate group is the only maximal self-conjugate subgroup of the symmetric group.* To prove it, we apply the same principle as above: If a self-conjugate subgroup H of the symmetric group contain a substitution h, it contains also all substitutions *similar* with h, since any two similar substitutions are conjugate under the symmetric group.

We confine ourselves again to the case $n = 5$, referring for the general case to Netto, §50.

The even substitutions lead exactly as in No. 44 to the alternate group. The substitution $h = (1\,2)$ leads to the symmetric group, since the latter can be generated by all the transpositions.

Finally, if H contain the substitution $h = (1\,3\,2\,4)$ or the substitution $(1\,3\,2)(4\,5)$, it contains also their squares, viz. $(1\,2)(3\,4)$ or $(1\,2\,3)$ respectively, and consequently the alternate group.

All different types of substitutions being thus exhausted, the alternate group is the only self-conjugate subgroup of the symmetric group (besides the symmetric group and the group 1).

46. We are now able to answer the question proposed at the end of No. 32; from the theorems of No. 37 and 42 we deduce the result:

In order that it be possible to choose the functions $\xi, \eta, \ldots . V$ of No. 31 such that *all the resolvents of the chain* (4) of No. 31 become *binomial equations* of prime degrees, it is necessary and sufficient that

1). All the indices $\lambda, \mu, \ldots . \rho$ are *prime numbers.*

2). In the series of groups

$$G_{n!},\ H,\ I \ldots . M,\ 1 \tag{1}$$

each group is a *self-conjugate subgroup* of the group immediately preceding it.

Under these conditions this series of groups (1) is precisely what we have defined as a series of composition of the symmetric group, since a self-conjugate subgroup of prime index is always a maximal self-conjugate subgroup, and therefore the above criterion may also be expressed in this form:

The necessary and sufficient condition for a chain of binomial resolvent equations is that all the factors of composition of the symmetric group be prime numbers.

Now these factors are, according to No. 43 and 44,

For $n = 4$: $2, 3, 2, 2$;

for any other n: $2, \frac{n!}{2}$.

Hence the above condition is satisfied for $n = 3$ and $n = 4$, but not for $n > 4$.

However, it would be erroneous to think that with this we have proved the impossibility of solving, by radicals, the general equation of a higher than the fourth degree. To complete our proof we should have to show that the method proposed in No. 31 is *the only possible method*; to this effect we should have to establish the two following propositions due to Abel:

Every equation which is solvable by radicals can be reduced to a chain of binomial equations of prime degrees, and

The roots of these binomial equations are expressible as rational functions of the roots of the given equation (see Netto, §201–210).

I omit, however, to enter here upon the proof of these theorems, since they have been superseded by Galois' theory of the solution of equations by radicals, in connection with which we shall have to reconsider the same questions from a more general point of view in the second part of this memoir.

47. But still I may briefly indicate already here how it happens that certain *special* equations of a higher degree are solvable by radicals, though the general equation be not solvable.

In the case of the general equation the symmetric functions are the only rational functions of the roots which are rationally expressible in terms of the coefficients, and consequently we must, in the series of groups of No. 31, start from the symmetric group.

In the case of special equations, on the contrary, it may happen that besides the symmetric functions some asymmetric function ϕ of the roots is rationally expressible in terms of the coefficients; in this case we need only to start from the group G to which ϕ belongs; and if the factors of composition of this group G are all prime, we can descend by the method of No. 31 from the function ϕ through a chain of binomial equations of prime degrees to an $n!$ valued function V, and the given equation is solvable by radicals.

But before all this can be established rigorously, a number of difficulties have to be removed, which arise the very moment we pass from the general equation to a special equation (see below, No. 55).

§10.—*Groups of Operations.*

48. The notion of a group as defined in No. 13 for the special case of substitutions, may be extended to any operations for which some definition of a product can be given.

To illustrate it, let us consider *the rotations of a rigid body about a fixed point;* let S be a first rotation through a given angle round a given axis, fixed in space and passing through the fixed point, S' another rotation of the same kind; then the successive application of first S, then S' is equivalent to one single rotation which is called the *product* SS' of the two rotations S and S' (see Thomson and Tait, Natural Philosophy, art. 95), and a system of rotations is said to form a *group*, if the product of any two of its rotations belongs itself to the system.

From this definition it is evident that those rotations which leave a regular polyedron congruent with its original position ("mit sich selbst zur Deckung bringen"), form a group.

In the case of a *regular tetraedron*, for example, there are $N = 12$ such rotations: The identical rotation (angle zero);

four rotations through an angle of $\frac{2\pi}{3}$, each round an axis passing through one of the corners and the middlepoint of the opposite face;

four rotations round the same axes, but through an angle of $\frac{4\pi}{3}$; these eight rotations have the period 3.

Finally, three rotations through an angle π round an axis passing through the middlepoints of two opposite edges, having the period 2.

These twelve rotations form a group called the *tetraedron-group.*

49. Most of the definitions and propositions on substitution-groups given in the foregoing paragraphs still hold for groups of any operations. For instance, those rotations of the tetraedron-group G which leave one of its *corners* unaltered —which we shall denote by ψ in order to show the complete analogy with the developments in No. 23 and 35—form a *subgroup* H *of the tetraedron-group* of

---

* References concerning §10: Jordan, No. 54-59, 76-81; Netto, §80-84.

index $\nu = 4$; it is a cyclic group consisting of the different powers of one of the rotations of period 3.

If operated upon by all the rotations of G, the corner ψ takes four different positions, viz. it comes to coincide successively with the four corners

$$\psi_1 = \psi, \ \psi_2, \ \psi_3, \ \psi_4$$

of the tetraedron, which for this reason are said to be *conjugate points* with respect to the tetraedron-group.

If g_α denote a rotation of G which brings the corner ψ to the place occupied, before the rotation, by the corner ψ_α, then the corner ψ_α remains unaltered by the subgroup

$$H_\alpha = g_\alpha^{-1} H g_\alpha,$$

which is said to be conjugate with H under G.

When the tetraedron is operated upon by a rotation of G, the four corners undergo a certain substitution; thus we obtain, as in No. 38, a *group* Γ *of substitutions among the letters* $\psi_1, \psi_2, \psi_3, \psi_4$ *isomorphic* with G; and since the rotation 1 is the only one that leaves all four corners at the same time unaltered, Γ is of the same order 12 as G and the isomorphism is *holoedric* (No. 39). Γ is therefore the *alternate group* between the four letters $\psi_1, \psi_2, \psi_3, \psi_4$ (No. 16).

In a similar way the consideration of an *edge* leads to a cyclic subgroup of order 2, and a substitution-group between the six edges, holoedrically isomorphic with G.

The consideration of the *straight line joining the middlepoints of two opposite edges* affords an example of a self-conjugate subgroup. For there are three such lines conjugate under G, all of which remain unaltered by the same subgroup of G, viz. the so-called "Vierergruppe" (Klein), consisting of the rotation 1 and the three rotations of period 2; the "Vierergruppe" is therefore a self-conjugate subgroup of the tetraedron-group.

Analogous considerations can be applied to the other regular polyedra:

The *Octaedron-group* is of order $N = 24$, and is holoedrically isomorphic with the symmetric group of four letters; the cube, being the polar figure of the octaedron, belongs to the same group.

The *Icosaedron-group* is of order $N = 60$, and is holoedrically isomorphic with the alternate group of five letters; the pentagon dodecaedron belongs to the same group.

To these groups may be added the *Cyclic groups* which leave the regular pyramids unaltered, and the *Diedron-groups* which leave the regular double pyramids unaltered (see Klein, Vorlesungen über das Ikosaeder, I, 1).

50. Another example of groups of operations is intimately connected with these groups of rotations. Let us, in fact, circumscribe about the polyedron under consideration, a sphere invariably connected with it: the points of the sphere may be analytically represented by the values of a complex variable z; to this effect we assume a system of rectangular coordinates X, Y, Z, fixed in space, with the origin in the middlepoint of the polyedron, and project the points of the sphere from the point of intersection of the positive Z-axis with the sphere ("North-pole") upon the XY-plane ("Plane of the equator"). X, Y being the coordinates of the projection of a point P of the sphere, the point P is represented by the complex quantity

$$z = X + iY.$$

If, now, by a rotation of the sphere about its middlepoint, the point P is brought into a new position P' represented by the complex quantity z', then z' can be expressed as a linear function of z:

$$z' = \frac{az + b}{cz + d},$$

the coefficients a, b, c, d being constant quantities, independent of the position of the point P (see Klein, l. c. I, 2).

If, then, the *product* of two such linear substitutions is defined as the linear substitution formed by combining them in the usual way, it is easily seen that corresponding to every group of rotations we obtain a group of linear substitutions holoedrically isomorphic with the group of rotations.

In the case of the tetraedron, for example, if we choose the lines joining the middlepoints of the three pairs of opposite edges as the axes of the system of coordinates, we obtain the following group of linear substitutions:

$$z' = \pm z, \ \pm \frac{1}{z}, \ \pm i.\frac{z+1}{z-1}, \ \pm i.\frac{z-1}{z+1}, \ \pm \frac{z+i}{z-i}, \ \pm \frac{z-i}{z+i}.$$

51. Thus we find, in connection with each regular polyedron, a series of groups of operations, all holoedrically isomorphic among themselves: the group of rotations, various groups of substitutions (permutations), finally, a group of

linear substitutions; and to these we may further add a group of quaternions, since every rotation may be represented by the versor of a quaternion.

All these groups are so intimately connected among themselves that they appear but as different forms of one and the same group *in abstracto.* (Compare different quantics which can be derived from one another by linear transformation.)

In fact, *two holoedrically isomorphic groups of operations G and Γ have all their most important properties in common.* They are of the same order; they have the same multiplication-table; that is, if in one group, $gg' = g''$, then the corresponding operations γ, γ', γ'' respectively of the other group satisfy the same relation $\gamma\gamma' = \gamma''$. Hence it follows that if any relation exists between any number of operations of G, the same relation exists also between the corresponding operations of Γ. In particular, two corresponding operations are of the same period; further, if g and g' are conjugate operations of G, then the corresponding operations γ and γ' are conjugate under Γ, etc.

To every subgroup H of G corresponds a subgroup H of Γ of the same order; and if H be self-conjugate under G, then also H is self-conjugate under Γ. Hence to a series of composition of G corresponds a series of composition of Γ.

52. Let, now, a, b, ... k denote a system of *generating operations* (No. 19) for the group G; then there exist, in general, numerous relations between them. It is always possible to select in various ways a number of these relations, sufficient and necessary to derive from them the multiplication-table of the group; such a set of relations is called a *system of fundamental relations.*

Example: The symmetric group of three letters can be generated by two substitutions (No. 8):

$$a = (1\,2\,3) \text{ and } c = (2\,3) \tag{1}$$

with the fundamental relations

$$a^3 = 1,\ c^2 = 1,\ (ac)^2 = 1. \tag{2}$$

The group is

$$1,\ a,\ b = a^2,\ c,\ d = ac,\ e = a^2c; \tag{3}$$

the value of any product can be found by means of the relations (2); for instance,

$$de = ac.a^2c,$$

but from (2) follows

$$aca = c, \quad cac = a^2,$$

hence

$$de = c.ac = a^2 = b,$$

in accordance with $(1\,3)(1\,2) = (1\,3\,2)$.

Now, if $\alpha, \beta, \ldots. \varkappa$ are the operations of the group Γ which correspond to the operations $a, b, \ldots. k$ respectively, then $\alpha, \beta, \ldots. \varkappa$ form a system of generating operations for the group Γ and satisfy exactly the same set of fundamental relations.

Conversely: Suppose two groups G and Γ are generated by the same number of generating operations $a, b, \ldots. k$ and $\alpha, \beta, \ldots. \varkappa$ respectively, satisfying the same fundamental relations; if, then, we coordinate a with α, b with β and so on, and besides every product

$$a^{\mu} b^{\nu} \ldots. a^{\mu'} b^{\nu'} \ldots.$$

with the similar product

$$\alpha^{\mu} \beta^{\nu} \ldots. \alpha^{\mu'} \beta^{\nu'} \ldots.,$$

then the correspondence thus established between the two groups is one of holoedric isomorphism.

Hence it follows that the group *in abstracto* of which various holoedrically isomorphic groups are but different forms (No. 51), may be *defined by a system of generating operations with a set of fundamental relations between them.*

Examples: 1). Tetraedron-group:

$$S^3 = 1, \quad T^2 = 1, \quad (ST)^3 = 1$$

(for instance, $S = (x_2 x_3 x_4)$, $T = (x_1 x_2)(x_3 x_4)$).

2). Octaedron-group:

$$S^4 = 1, \quad T^2 = 1, \quad (ST)^3 = 1$$

(for instance, $S = (x_1 x_2 x_3 x_4)$, $T = (x_1 x_2)$).

3). Icosaedron-group:

$$S^5 = 1, \quad T^2 = 1, \quad (ST)^3 = 1.$$

(for instance, $S = (x_1 x_2 x_3 x_4 x_5)$; $T = (x_2 x_3)(x_4 x_5)$).

But a remark is necessary concerning this definition of a group; if we assume at random a set of fundamental relations between a number of generating operations, we will always define a group, but in general the group will contain an *infinite number of different operations;* for instance, the group generated by two generating operations S, T with the relations

$$S^n = 1, \quad T^2 = 1, \quad (ST)^3 = 1$$

will be finite only if $n \overline{\leqq} 5$, infinite in all other cases.

53. *Every finite group of operations is holoedrically isomorphic with a regular substitution-group;* this group is given by the multiplication-table of the group. For if

$$S_1, S_2, \dots . S_N \tag{1}$$

are the operations of the given group G, and S any one of them, then the N products

$$SS_1, SS_2, \dots . SS_N \tag{2}$$

are a permutation of the operations (1); and if we coordinate with every operation S of G the substitution

$$\sigma = \begin{pmatrix} S_1 & S_2 & \dots . & S_N \\ SS_1 & SS_2 & \dots . & SS_N \end{pmatrix} \tag{3}$$

between the N letters S_1, S_2, ... S_N, we obtain a regular substitution-group Γ (No. 24), which is holoedrically isomorphic with the given group G; it is called the *regular form of the given group* G (Dyck).

References concerning groups of operations:

Cayley: On the Theory of Groups. Phil. Mag. 4th Series. Vol. 7 and 18.
American Journal of Math., Vol. 1 and 11.
Dyck: Gruppentheoretische Studien, Math. Annalen, Bd. 22.
Klein: Vorlesungen über das Ikosaeder, I, 1.

54. In concluding we give an enumeration of some of the most important classes of groups of operations:

1). Groups of *Substitutions* (permutations).

2). Groups of *Rotations.*

See above, No. 48; groups of *movements* in general have been studied by Schönfliess, Math. Ann. Bd. 28 and 29.

3). Groups of *non-homogeneous linear substitutions* of one variable:

$$z' = \frac{az + b}{cz + d}, \tag{1}$$

the only *finite groups* are those which represent analytically the groups of rotations enumerated in No. 48; see Klein, Ikosaeder, p. 115, where a list of references is given.

The general theory of "discontinuous" *infinite groups* has been developed by Poincaré in a series of memoirs in the Acta Math., Vol. 1, 3, 4, 5.

An important special case is the group of all the linear substitutions of the form (1) in which the coefficients are *integers* satisfying the relation

$$ad - bc = 1.$$

See Dedekind, Borchardt's Journal, Bd. 83; Klein, Ueber die Transformation der elliptischen Functionen, Math. Annalen, Bd. 14.

4). Groups of *homogeneous linear substitutions* of several variables:

$$z'_\alpha = a_{\alpha_1} z_1 + a_{\alpha_2} z_2 + \dots a_{\alpha_n} z_n. \tag{2}$$

See Jordan, Cours d'analyse III, No. 156; as to finite groups in particular, see Klein, Ikosaeder, p. 123, where a list of references is given.

5). An essentially different class of groups are *Lie's transformation-groups;* such a group is for instance the entire system of all the linear transformations

$$x' = \frac{a_1 x + a_2}{a_3 x + a_4},$$

the coefficients taking all possible values (see Lie, Transformationsgruppen, Math. Ann. Bd. 16, and Lie, Theorie der Transformationsgruppen, Leipzig, 1888).

SECOND PART.

GALOIS' THEORY OF ALGEBRAIC EQUATIONS.

§11.—*Galois' Resolvent.*

55. Hitherto we have always been dealing with the *general equation* of the n^{th} degree; that is to say, we have considered the coefficients $c_1, c_2 \dots . c_n$, and consequently also the roots $x_1, x_2 \dots . x_n$, as indeterminate quantities. Accordingly we have regarded two rational functions of the roots as equal only when they were identical for all sets of values of the x's (see No. 7).

But if, on the contrary, the x's are the roots of a given *special equation*, we shall have to consider two rational functions of the roots as equal when their *numerical values* are equal, and it may happen that the numerical value of a rational function ψ of the roots remains unaltered by a substitution which changes the form of the function. For instance, in the case of the equation

$$x^4 + x^3 + x^2 + x + 1 = 0$$

whose roots are the imaginary fifth roots of unity:

$$x_1 = \omega, \quad x_2 = \omega^2, \quad x_3 = \omega^4, \quad x_4 = \omega^3,$$

where $\omega = e^{\frac{2\pi i}{5}}$,

we have $x_1^2 x_2 = x_3^2 x_1$, viz. $= \omega^4$,

though the two functions $x_1^2 x_2$ and $x_3^2 x_1$ are different in form.

In such a case it would not be allowed to apply Lagrange's theorem to the function ψ because the denominator Δ_ψ vanishes (see No. 28).

Further, those substitutions which leave unaltered the numerical value of a rational function of the roots of a special equation do not, in general, form a group. Thus in the above example the numerical value of the function $x_1^2 x_2$ remains unaltered by the substitutions

$$1; \ (x_3 x_4); \ (x_1 x_3 x_2); \ (x_1 x_3 x_4 x_2),$$

which evidently do not form a group.

In a similar way nearly every one of our theorems on asymmetric functions becomes either entirely wrong, or is true only under certain restricting conditions, if applied to rational functions of the roots of a special equation.

These difficulties which arise in passing from the general equation to a special equation are due to the fact that the so-called general equation is not the true general case, but in truth a very special one; and our next task is to generalize the theorems on asymmetric functions in such a manner that they hold for any given equation without any restrictions (see below No. 67).

56. We consider an equation of the n^{th} degree:

$$f(x) = x^n - c_1 x^{n-1} + c_2 x^{n-2} \dots \pm c_n = 0 \tag{1}$$

whose coefficients we suppose to be rational functions, with integral coefficients, of a number of *known quantities*, determinate or indeterminate, which we denote by

$$\mathfrak{R}', \ \mathfrak{R}'', \ \mathfrak{R}''' \dots . \tag{2}$$

Any quantity which is expressible as a rational function, with integral coefficients, of these quantities (2), is called *rationally known* or simply *rational.*[*]

By a *rational function* or a *rational relation* we shall always understand a rational function or relation whose coefficients are rational quantities.

---

[*] The entire system of all these "rational quantities" are said to constitute the "*domain of rationality* ($\mathfrak{R}'$, $\mathfrak{R}''$, ...)" ("Rationalitätsbereich," Kronecker); the simplest domain of rationality consists of all rational numbers; it is called the domain $\mathfrak{R} = 1$.

All interesting applications of Galois' theory come under one of the two following cases:

1). There are only a *finite number* of known quantities (2), and all of them are *algebraic* quantities; that is to say, such an $\mathfrak{R}$ is either an *algebraic number* satisfying an algebraic equation with integral coefficients, or an *indeterminate quantity* or an *algebraic function* satisfying an algebraic equation whose coefficients are rational functions with integral coefficients of some indeterminate quantities.

Examples:

$$x^n + x^{n-1} + \dots + x + 1 = 0; \quad (\mathfrak{R} = 1),$$

$$x^3 - \frac{-1+\sqrt{-7}}{2} x^2 + \frac{-1-\sqrt{-7}}{2} x - 1 = 0; \quad (\mathfrak{R}' = \sqrt{-7}).$$

Modular equation between $x = v$ and $\mathfrak{R}' = u$. Equation of the degree n^2 for the division of $\operatorname{sn} u$:

$$x = \operatorname{sn}\frac{u}{n}; \ \mathfrak{R}' = k^2; \ \mathfrak{R}'' = \operatorname{sn} u; \ \mathfrak{R}''' = \sqrt{(1-\mathfrak{R}''^2)(1-\mathfrak{R}'\mathfrak{R}''^2)}$$

(see Kronecker, Grundzüge einer arithmetischen Theorie der algebraischen Grössen, Borchardt's Journal, Bd. 92; and Molk, Sur la notion de la divisibilité, etc., Acta Math., Vol. 6, pg. 20, 35, 40).

2). *All constant quantities* are considered as being known, and besides a finite number of variable quantities $\mathfrak{R}'$, $\mathfrak{R}'' \dots \mathfrak{R}^{(\mu)}$, partly independent variables, partly algebraic functions, in the sense of the theory of functions, of some independent variables; we shall denote such a domain by

$$(\text{Const.}, \mathfrak{R}', \mathfrak{R}'' \dots \mathfrak{R}^{(\mu)}).$$

"Two rational functions of the roots are *equal*" will be understood to mean: *a*). If the known quantities (2) are all determinate: "*equal in numerical value.*" *b*). If some of the known quantities are indeterminate: "*equal for all values of these indeterminate quantities.*"

"*Different*" or "*distinct*" means: not equal, in this sense.

Accordingly we shall say a rational function ϕ of the roots *remains unaltered* by a substitution s, if the new function ϕ_s is equal, in this sense, to ϕ.

All these definitions are generalizations of our former ones; in fact, the so-called *general equation* is comprised as a special case in the above assumptions; the known quantities are, in this case, the n indeterminate coefficients

$$\mathfrak{R}', \mathfrak{R}'' \dots \mathfrak{R}^{(n)}$$

and the equation is then

$$x^n + \mathfrak{R}'x^{n-1} + \mathfrak{R}''x^{n-2} + \dots + \mathfrak{R}^{(n)} = 0.$$

57. An integral function $F(x)$ or an equation $F(x) = 0$, whose coefficients are rational quantities, is said to be *reducible* (in the domain $(\mathfrak{R}'\mathfrak{R}''\dots)$) if it can be decomposed into factors of a lower degree whose coefficients are themselves rational quantities; *irreducible* if no such decomposition is possible.*

A reducible integral function can always, and only in one way, be decomposed into irreducible factors (see Kronecker, l. c. §§1–4, and Molk, l. c. Chap. II).

If one root of an irreducible equation $F(x) = 0$ satisfies at the same time another equation $G(x) = 0$ whose coefficients are likewise rational quantities, then ALL *the roots of the irreducible equation satisfy the second equation* (see Serret, No. 100).

Hence, if two irreducible equations have one root in common, they are altogether identical.

58. To the assumptions of No. 56 concerning the nature of the coefficients of the given equation

$$f(x) = 0, \tag{1}$$

we add one more hypothesis, viz. that *its n roots $x_1, x_2, \dots x_n$ are all distinct.*

---

*In this definition we include expressly the case where some of the quantities $\mathfrak{R}', \mathfrak{R}'' \dots$ do not explicitly enter into the coefficients; the notion of irreducibility is therefore *relative.* For instance, the equation

$$x^4 + x^3 + x^2 + x + 1 = 0$$

is irreducible in the domain $\mathfrak{R} = 1$; but the coefficients may as well be considered as belonging to the domain $(\sqrt{5})$, and in this case the equation is reducible, since it may be written

$$\left(x^2 + \frac{1+\sqrt{5}}{2}x + 1\right)\left(x^2 + \frac{1-\sqrt{5}}{2}x + 1\right) = 0.$$

a). Under these conditions *it is always possible to construct a rational function of the roots which takes $n!$ different values* if operated upon by all the $n!$ substitutions between the letters $x_1, x_2, \ldots . x_n$.

Such a function is, for instance,

$$V_1 = m_1x_1 + m_2x_2 + \ldots . m_nx_n, \tag{3}$$

if the coefficients m be properly chosen.

For two values V_a and V_b derived from V_1 by two different substitutions a and b respectively, cannot be equal for all values of the parameters m, since all the roots x are supposed to be distinct. Hence it is always possible to choose for the m's such rational quantities which satisfy none of the $\frac{n!\,(n!-1)}{2}$ relations of the form $V_a = V_b$; V_1 is then in fact an $n!$-valued function.

From an equation of the form

$$V_{a'} = V_a$$

we may then always infer $a' = a$.

b). *It is always possible to construct a rational function of the roots of* (1) *which remains unaltered by the substitutions of any given substitution-group*

$$H = [1,\ a,\ b, \ldots . k]$$

between the letters $x_1, x_2, \ldots . x_n$.

Such a function is for instance

$$\psi = (r - V_1)(r - V_a)(r - V_b) \ldots . (r - V_k),$$

r being a properly chosen rational quantity (compare No. 18, and Jordan, No. 351).

59. *Any rational function of the roots of the given equation* (1) *is rationally expressible in terms of such an $n!$-valued function* V_1:

$$\phi(x_1, x_2, \ldots . x_n) = \Phi(V_1); \tag{4}$$

moreover, *the function* ϕ_a derived from ϕ by any substitution a between the letters $x_1, x_2, \ldots . x_n$, *is the same function* Φ *of* V_a:

$$\phi_a(x_1, x_2, \ldots . x_n) = \Phi(V_a). \tag{5}$$

Proof: We consider first the x's as indeterminate quantities; in this case (4) follows from Lagrange's theorem (No. 27) and (5) is a self-evident consequence of (4). Afterwards we replace the indeterminate quantities x by the roots of the given equation, which we may safely do, since the discriminant Δ_{V_1} is not zero (compare No. 28); the coefficients of the rational function Φ are then changed into rational quantities of our domain $(\mathfrak{R}', \mathfrak{R}'' \ldots)$*

In particular, *the roots of the given equation are rationally expressible in terms of* V_1:

$$x_1 = \psi_1(V_1), \quad x_2 = \psi_2(V_1) \ldots . x_n = \psi_n(V_1). \tag{6}$$

60. The $n!$ conjugate values of the function V_1 are the roots of a resolvent equation of the degree $n!$ (No. 26),

$$F(V) = 0, \tag{7}$$

whose coefficients are rational quantities. Let now $F_0(V)$ be that irreducible factor† of $F(V)$ which has the root $V = V_1$; *the irreducible equation*

$$F_0(V) = 0 \tag{8}$$

is then called Galois' Resolvent of the given equation (1).

Let $N(\overline{\gtrless} n!)$ be its degree. Its roots are contained among the roots of (7) and are therefore some of the conjugate values of V_1; hence they are rationally expressible in terms of V_1, according to No. 59; thus we have the theorem:

All the roots of Galois' resolvent are rationally expressible in terms of one of them.

The solution of the given equation (1) is equivalent to the determination of one root V_1 of Galois' resolvent, since all the roots of (1) are rationally expressible in terms of V_1 (*Galois' Principle;* compare No. 31).

§12.—*Group of an Equation.*

61. Let now

$$V_1, \ V_a, \ V_b, \ldots . V_l \tag{9}$$

be the N roots of Galois' resolvent (8), derived from V_1 by the substitutions

$$1, \ a, \ b, \ldots . l \tag{10}$$

respectively.

---

* The second part of the theorem is only true if no reductions are made in the expression of the rational function Φ_1 (by means of the irreducible equation $F_0(V_1) = 0$ of No. 60), after the indeterminate x's have been replaced by the roots of (1).

† With respect to the domain of rationality $(\mathfrak{R}', \mathfrak{R}'' \ldots)$. If $F(V)$ itself should be irreducible, we have simply $F_0(V) = F(V)$.

These substitutions form a group; to prove it we have but to show that if V_a and V_b are any two roots of (8), then also V_{ab}, derived from V_1 by the product ab, will be a root of (8).

V_a being a root of (8), we have

$$F_0(V_a) = 0.$$

Now, according to No. 60, V_a is expressible as a rational function of V_1, say

$$V_a = \theta(V_1), \tag{11}$$

therefore we have

$$F_0[\theta(V_1)] = 0.$$

The root V_1 of the irreducible equation (8) satisfies therefore at the same time the equation

$$F_0[\theta(V)] = 0, \tag{12}$$

whose coefficients are rational quantities, consequently (No. 57) all the roots of (8) satisfy (12), in particular also the root V_b; that is,

$$F_0[\theta(V_b)] = 0.$$

But from (11) follows, according to the lemma of No. 59,

$$V_{ab} = \theta(V_b); \tag{13}$$

hence V_{ab} is also a root of Galois' resolvent (8), and consequently the product ab is itself one of the substitutions (10). Thus we have proved the theorem:

The N substitutions by which the N roots of Galois' resolvent can be derived from one of them, V_1, form a group.

This group is called *the group of the given equation* (1) *with respect to the domain of rationality* ($\mathfrak{R}'$, $\mathfrak{R}''$, ...);* we denote it by G.

62. The group G of the given equation (1) possesses the following two fundamental properties:

A. *Every rational function of the roots of $f(x) = 0$ which remains unaltered by all the substitutions of the group G, is rationally known.*

B. *Every rational function of the roots of $f(x) = 0$ which is rationally known remains unaltered by all the substitutions of G.*

---

* It may, however, be remarked that this theorem as well as the lemmas of No. 59 can be proved directly without recurring to the case of indeterminate x's, and this would indeed be more in accordance with the spirit of Galois' theory. The proofs may be found in Serret, No. 502, 504.

Proof: Let $\phi = \phi(x_1, x_2, \ldots . x_n)$ be a rational function of the roots; we express it in terms of V_1:

$$\left.\begin{array}{l} \phi = \Phi(V_1); \\ \text{according to the lemma (5) of No. 59, we have then} \\ \phi_a = \Phi(V_a), \\ \phi_b = \Phi(V_b), \\ \ldots\ldots\ldots\ldots \\ \phi_l = \Phi(V_l), \end{array}\right\} \qquad (14)$$

Φ denoting throughout the same rational function.

Let us now first suppose, as in A, that

$$\phi = \phi_a = \phi_b = \ldots . = \phi_l;$$

then we obtain, by adding the equations (14),

$$\phi = \frac{1}{N}\left[\Phi(V_1) + \Phi(V_a) + \Phi(V_b) \ldots . + \Phi(V_l)\right].$$

The expression on the right-hand side is a symmetric function of all the N roots of Galois' resolvent

$$F_0(V) = 0, \qquad (8)$$

and therefore rationally expressible in terms of the coefficients of this equation, which, in their turn, are rational quantities. Hence ϕ itself is rationally known.

Q. E. D.

To prove the conversion B, let us suppose that ϕ is rationally known,

$$\phi(x_1, x_2, \ldots . x_n) = \text{Rat.}(\mathfrak{R}', \mathfrak{R}'', \ldots .) = r,$$

On account of (14) this relation may be written

$$\Phi(V_1) - r = 0.$$

One root of the irreducible equation (8), viz. $V = V_1$, satisfies therefore the equation

$$\Phi(V) - r = 0, \qquad (15)$$

whose coefficients are rational quantities; hence (No. 57) all the roots of (8) must satisfy (15); that is,

$$\Phi(V_1) = \Phi(V_a) = \Phi(V_b) \ldots . = \Phi(V_l) = r,$$

or on account of (14),

$$\phi = \phi_a = \phi_b \;\ldots\ldots = \phi_l = r;$$

that is, ϕ remains unaltered by all the substitutions of G. Q. E. D.

Remark: The proposition B may also be expressed in the following form, which is preferable in most applications:

B′. *Any rational relation between the roots remains true if operated upon by any substitution of the group G.*

63. *These two properties are characteristic of the group of an equation;* that is to say, if the two propositions A and B hold for a group G', then G' is identical with G.

a). Let us first suppose we know of the group

$$G' = [1,\ a',\ b' \ldots\ldots m']$$

that every rational function of the roots of (1) which remains unaltered by all the substitutions of G' is rationally known.

We form the function

$$(V - V_1)(V - V_{a'}) \ldots\ldots (V - V_{m'}) = F'(V);$$

its coefficients being symmetric functions of $V_1,\ V_{a'} \ldots\ldots V_{m'}$, remain unaltered by G' and are therefore, according to our hypothesis, rational quantities. Hence follows (No. 57) that $F'(V)$ is divisible by the irreducible function $F_0(V)$ and therefore the roots of $F_0(V)$ must all be contained among the roots of $F'(V)$; hence we have the result:

If for a group G' the proposition A holds, then G' must contain the group G of the equation, or

The group of the equation is the smallest group for which the proposition A *holds.*

b). Let us now suppose we know of the group

$$G'' = [1,\ a'',\ b'' \ldots\ldots p'']$$

that every rational relation between the roots remains true if operated upon by all the substitutions of G''. Applying this hypothesis to the relation $F_0(V_1) = 0$ we obtain

$$F_0(V_{a''}) = 0,\ \ F_0(V_{b''}) = 0 \ldots\ldots F_0(V_{p''}) = 0;$$

consequently the values

$$V_1,\ \ V_{a''},\ \ V_{b''} \ldots\ldots V_{p''}$$

must be contained among the roots of $F_0(V) = 0$; hence

If for a group G'' the proposition B holds, then G'' must be contained in G, or

The group of an equation is the largest group for which the proposition B *holds.*

c). Now, if for the same group, G', the two propositions A and B hold, then G' must at the same time contain G and be contained in G, which is only possible if $G' = G$. Q. E. D.

Hence the two fundamental properties may be used as a *new definition* of the group of an equation; it has the advantage of showing at once that the group of an equation is independent of the choice of the $n!$-valued function V_1.

64. If the coefficients of the given equation contain some indeterminate parameters, the group of the equation may be defined still in an entirely different way.

Let us, in order to fix the ideas, consider an equation of the n^{th} degree

$$f(x;\ t) = 0, \tag{1}$$

whose coefficients are rational functions, with any constant coefficients, of one indeterminate parameter t.

The n roots $x_1, x_2, \ldots . x_n$ of (1) are algebraic functions of t. If, then, the parameter t, which we represent as usual by a point in a t-plane, describes a closed curve in its plane, starting from some fixed initial position, the n roots are only interchanged among themselves. Hence if the point t describes all possible closed curves, the letters $x_1, x_2, \ldots . x_n$ undergo a series of different substitutions, which are easily seen to form a group, called the *monodromy-group* of the equation (1) with respect to the parameter t. Now, this group can be proved to be identical with the group of the equation (1), as defined in No. 61, with respect to the domain of rationality (Const., t) which consists (see No. 56, note) of all the rational functions with any constant coefficients, of the parameter t (see Jordan, No. 390).

If, in particular, the coefficients of (1) are rational functions, with *integral* coefficients of t, there exist at the same time a monodromy-group and an "algebraic group" of the equation (1), the former referring to the domain of rationality (Const., t), the latter to the domain (t).

In this case *the monodromy-group is always a self-conjugate subgroup of the algebraic group* (see Jordan, No. 391).

Moreover, there exists always an algebraic number ε such that the monodromy-group is identical with the group of (1) with respect to the domain (ε, t) (see Jordan, No. 391).

Example:

$$f(x;t) = x^n - t = 0 \qquad (n \text{ prime}).$$

The n roots may be written

$$x_0,\ x_1 = \omega x_0,\ x_2 = \omega^2 x_0, \ldots . x_{n-1} = \omega^{n-1} x_0,$$

ω denoting a primitive n^{th} root of unity; the monodromy-group is the cyclic group consisting of the n different powers of the substitution

$$(x_0, x_1, x_2, \ldots . x_{n-1}).$$

The algebraic group is the so-called "metacyclic group" (see below, No. 79), which, in fact, contains the cyclic group as a self-conjugate subgroup.

The quantity ε is in this case ω; in the domain (ω, t) the equation is, in fact, a "cyclic equation" (see below, No. 73).

65. *If an equation is irreducible, its group is transitive, and vice versa.* For if the group G of the equation $f(x) = 0$ is intransitive (No. 24), connecting transitively only the roots $x_1, x_2, \ldots . x_m\,(m < n)$, then any symmetric function of these m roots remains unaltered by all the substitutions of G and is, consequently, rationally known (No. 62, A); the product $(x - x_1)(x - x_2) \ldots . (x - x_m)$ is therefore a rational divisor of $f(x)$ and $f(x)$ is reducible.

Conversely, if $f(x)$ is reducible and $f_0(x) = (x - x_1)(x - x_2) \ldots . (x - x_m)$ a rational factor of $f(x)$, then the rational relation $f_0(x_1) = 0$ remains true if operated upon by any substitution of G (No. 62, B′); therefore no substitution of G can replace x_1 by one of the roots $x_{m+1}, \ldots . x_n$; that is to say, G is intransitive.

Thus both parts of our proposition are proved.*

§13.—*Theorems on Asymmetric Functions of the Roots.*

66. In the case of the so-called "general" equation

$$x^n + \mathfrak{R}' x^{n-1} + \mathfrak{R}'' x^{n-2} + \ldots . + \mathfrak{R}^{(n)} = 0,$$

the $\mathfrak{R}$'s being indeterminate quantities (see No. 56), the symmetric functions are the only rational functions of the roots which are rationally known.

---

* References concerning §11 and 12: Galois, Journal de mathématiques pures et appliquées, Vol. XI (1846); Serret, No. 502, 504, 577, 578, 579; Jordan, No. 348-357; Netto, §221, §223; Bachmann, Ueber Galois' Theorie der algebraischen Gleichungen, Math. Ann. 18.

For in any relation of the form

$$\phi(x_1, x_2, \ldots\ldots x_n) = \text{Rat.}(\mathfrak{R}', \mathfrak{R}'', \ldots\ldots \mathfrak{R}^{(n)}),$$

the right-hand side can be transformed into a symmetric function of $x_1, x_2, \ldots x_n$, and since the relation is understood to hold for all values of $\mathfrak{R}', \mathfrak{R}'', \ldots\ldots \mathfrak{R}^{(n)}$ (see No. 56, definition of "equal"), and consequently also for all values of $x_1, x_2, \ldots\ldots x_n$, ϕ must itself be a symmetric function.

Hence follows, according to No. 63, a), that *the group of the "general" equation is the symmetric group.*

Hence the fundamental theorem A (No. 62), if applied to the "general" equation, assumes the familiar form:

Every symmetric function of the roots is rationally expressible in terms of the coefficients.

67. In a similar way the theorems on asymmetric functions of n indeterminate quantities of §§3, 4 and 5 may be considered as special cases of more general theorems which hold for the roots of any given equation and in which the group of the equation takes the place of the symmetric group in the former case.

a). Thus the theorem of No. 13:

"Those substitutions (of the symmetric group) which leave a rational function of n indeterminate quantities $x_1, x_2, \ldots\ldots x_n$ unaltered, form a group," is a special case of the following:

Those substitutions OF THE GROUP *G of the equation $f(x) = 0$ which leave a rational function of its roots unaltered, form a group.*

We may repeat, word by word, the proof of No. 13, confining ourselves, however, exclusively to the consideration of substitutions of the group G, and replacing the truism:

"Every rational relation between the indeterminate quantities $x_1, x_2, \ldots x_n$ remains true if operated upon by any substitution," by the corresponding general theorem B′:

"Every rational relation between the roots of $f(x) = 0$ remains true if operated upon by any substitution *of the group* G of the equation."

Henceforward we shall say, the function ψ *belongs* to the group H (subgroup of G), if it remains unaltered by all the substitutions of H and by no other substitutions of G.

b). Modifying in the same way the conclusions of No. 23 and No. 26, and replacing the fundamental theorem on symmetric functions by the fundamental theorem A (No. 62), we find:

If ν be the index of H under G, then ψ takes ν different values

$$\psi_1 = \psi, \quad \psi_2, \ldots . \psi_\nu$$

if operated upon by all the substitutions of G.

These ν values are the roots of a resolvent equation of the ν^{th} degree

$$g(\psi) = 0$$

whose coefficients are rational quantities.

c). Further, *Lagrange's theorem* takes the form

If a rational function ϕ of the roots of $f(x) = 0$ remains unaltered by all those substitutions of the group G which leave another function ψ unaltered, then ϕ is rationally expressible in terms of ψ:

$$\phi = \text{Rat.}\,(\psi);$$

and the theorem *is true without exception,* for the denominator of Rat. (ψ) is now the square of the product of all the differences of the ν conjugate values of ψ *under* G, and is therefore not zero according to *b*) (compare No. 28).

Remark: In all these generalized theorems, the expressions "equal," "different," "unaltered" are understood in the sense of No. 56.

68. *Application to regular equations.* Let us consider an equation of the n^{th} degree

$$f(x) = 0 \tag{1}$$

whose group G is regular, that is (No. 24), transitive and of order n; such an equation is called a *regular equation.*

a). Since the group is supposed to be transitive, the equation (1) is *irreducible* (No. 65).

b). Since, besides, the group is of order n, the substitution 1 is the only substitution of G which leaves x_1 (or any other root) unaltered; x_1 "belongs" therefore to the group 1 (No. 67, *a*), and consequently *all the roots are rationally expressible in terms of any one of them,* for instance x_1:

$$x_2 = \theta_2(x_1), \quad x_3 = \theta_3(x_1) \ldots . x_n = \theta_n(x_1). \tag{2}$$

These two properties are *characteristic* of a regular equation.

For the irreducibility implies the *transitivity* of the group G; and from the relations (2) follows, with the aid of the fundamental theorem B′ (No. 62), that the substitution 1 is the only substitution of G which does not displace the letter x_1; hence, according to No. 24, the group G is indeed regular.

§14.—*Reduction of the Group by Adjunction.*

69. In all the preceding investigations we have been "operating in the domain of rationality,"

$$\mathfrak{R} = (\mathfrak{R}', \mathfrak{R}'', \ldots.),$$

to which the coefficients of our given equation

$$f(x) = 0 \tag{1}$$

were supposed to belong, and the definition of irreducibility and accordingly of the group G of the equation referred to this domain $\mathfrak{R}$.

Let us now suppose we had found, by solving some auxiliary equation, an irrational function ξ of the quantities $\mathfrak{R}', \mathfrak{R}'', \ldots.$; we may then, henceforth, consider also ξ as a known quantity, or, in the language of Galois and Kronecker, *adjoin it to our domain of rationality*, so that we obtain the enlarged domain:

$$R' = (\xi\,;\ \mathfrak{R}', \mathfrak{R}'', \ldots.).$$

The coefficients of (1) belong *a fortiori* also to the enlarged domain R' and we may therefore repeat all our former developments with respect to the domain R'.

The group G' of (1) with respect to the new domain is now defined by that factor $F_0'(V; \xi)$ of $F(V)$, rational and irreducible in the domain R', which has the root V_1 (No. 61). Since the function $F_0(V)$ of No. 61 and this irreducible function $F_0'(V; \xi)$ have the root V_1 in common, $F_0(V)$ must be divisible by $F_0'(V; \xi)$ (No. 57), and consequently G' must be a subgroup of G; in Galois' terms: "*by the adjunction of* ξ, *the group* G *of* (1) *is reduced to the subgroup* G'" (including, however, the case $G' = G$, which happens if $F_0(V)$ remains irreducible after the adjunction of ξ, so that $F_0'(V; \xi) = F_0(V)$; compare No. 57, note).

70. We consider first the case where the adjoined quantity is a rational function of the roots:

By the adjunction of a rational function ψ *of the roots* $x_1, x_2, \ldots. x_n$, *which belongs to a subgroup* H *of* G, *the group* G *of the equation is reduced precisely to the subgroup* H.

For any rational function ϕ of the roots which remains unaltered by all the substitutions of H is rationally expressible in terms of ψ according to Lagrange's theorem generalized (No. 67, c) and belongs therefore to the new domain

$$R' = (\psi;\ \mathfrak{R}',\ \mathfrak{R}'',\ \ldots .).$$

Conversely, any rational function ϕ of the roots which is rationally known in the domain R', remains unaltered by all the substitutions of H.

For the relation

$$\phi\,(x_1,\ x_2,\ \ldots .\ x_n) = \text{Rat.}\,(\psi\,(x_1,\ x_2,\ \ldots .\ x_n);\ \mathfrak{R}',\ \mathfrak{R}'',\ \ldots .)$$

remains true if operated upon by any substitution of G (No. 62, B′) and, *a fortiori*, of its subgroup H; but the substitutions of H leave ψ unaltered, and consequently, the whole right-hand side; therefore also ϕ remains unaltered by all the substitutions of H.

The group H satisfies therefore the two characteristic conditions of the group of (1) with respect to the domain R'.

71. The quantity ψ, which we have considered as known in the last No., is obtained by solving the resolvent equation (No. 67, *b*),

$$g\,(\psi) = 0$$

of the degree ν, if we denote again by ν the index of the subgroup H under G. *The group of this resolvent equation* (whose roots are the ν conjugate values $\psi_1,\ \psi_2,\ \ldots .\ \psi_\nu$ of ψ under G) *is the group* Γ, *isomorphic with* G, *of those substitutions which the* ψ*'s undergo when the* x*'s are operated upon by all the substitutions of* G (see No. 38).

For any rational function $R\,(\psi_1,\ \psi_2,\ \ldots .\ \psi_\nu)$ of the ψ's may at the same time be considered as a rational function of the x's:

$$R\,(\psi_1,\ \psi_2,\ \ldots .\ \psi_\nu) = r\,(x_1,\ x_2,\ \ldots .\ x_n);$$

and if R remains unaltered by all the substitutions of Γ, then r remains unaltered by all the substitutions of G, and vice versa. Hence the group Γ can easily be proved to possess the two fundamental properties A and B (No. 62), characteristic of the group of the equation $g\,(\psi) = 0$.

Corollaries: 1. Since the root ψ_1 can be changed by substitutions of G, and consequently also by substitutions of Γ into every one of the ν values $\psi_1,\ \psi_2,\ \ldots\ \psi_\nu$, Γ is transitive, and therefore *the resolvent* $g\,(\psi) = 0$ *is irreducible* (No. 65).

2). If the group H to which ψ "belongs" is a *self-conjugate* subgroup of G, then the resolvent is a *regular equation*[*] (No. 39).

3). If, in particular, H is a *maximum self-conjugate* subgroup of G, then the resolvent is a *regular and simple equation* (No. 39, *b*; 38, 43).

4). Finally, if H is a *self-conjugate* subgroup of *prime* index ν of G, then the resolvent is a *cyclic equation of prime degree* ν (No. 39, *c*).

5). Let us finally consider the case where the given equation $f(x) = 0$ is *irreducible* and the rational function ψ *contains only one single root:*

$$\psi = \psi(x_1).$$

In this case the group of (1) is transitive (No. 65), and the index of that subgroup I of G which does not displace x_1 is n (No. 24).

Now that subgroup H of G to which ψ belongs contains evidently the group I, and consequently the index ν of H under G, and therefore also *the degree of the irreducible resolvent equation* $g(\psi) = 0$, *is a divisor of* n.

72. An equation $f(x) = 0$ whose group G is composite (No. 43) is called a *composite equation.*

The solution of a composite equation can always be reduced to the solution of a chain of SIMPLE REGULAR *equations.*

For let $$G - H - I \ldots . M - 1$$

be a series of composition (No. 43) of the group G of the given equation; λ, μ, ... ρ the factors of composition and ϕ, ψ, ... χ, V rational functions of the roots belonging to the groups H, I, ... M, 1 respectively (see No. 58, *b*). Then ϕ is found by solving a resolvent equation of the degree λ, simple and regular with respect to the original domain (No. 71, 3).

By the adjunction of ϕ, the group G of the equation is reduced to the subgroup H (No. 70).

A second resolvent equation of the degree μ, simple and regular with respect to the new domain furnishes ψ, by the adjunction of ψ the group H of the equation is reduced to the subgroup I and so forth, and our proposition is proved.[†]

---

[*] The expressions "regular," "simple," "cyclic," etc., are transferred from the group Γ to the equation $g(\psi) = 0$; a regular equation is an equation whose group is regular, etc.

[†] References concerning §14: Jordan, No. 362, 372; Serret, No. 580, 583; Netto, §228.

§15.—*Cyclic or Abelian Equations.*

73. The equation

$$f(x) = 0 \tag{1}$$

is called a *cyclic equation* if its group G is the cyclic group consisting of the n different powers of a circular substitution, say

$$G = [1, s, s^2, \ldots . s^{n-1}],$$
$$s = (x_0, x_1, \ldots . x_{n-1}),$$

$x_0, x_1, \ldots . x_{n-1}$ denoting the n roots of (1).

The cyclic group G is regular; hence the equation (1) is *irreducible* and all its roots are rationally expressible in terms of one of them (No. 68), say, in particular, $x_1 = \theta(x_0)$.

This rational relation remains true if operated upon by all the substitutions of G (No. 62, B′), hence we obtain

$$x_1 = \theta(x_0),\ x_2 = \theta(x_1),\ x_3 = \theta(x_2) \ldots . x_{n-1} = \theta(x_{n-2}),\ x_0 = \theta(x_{n-1}), \tag{2}$$

or, if we denote

$$\theta[\theta(x_0)] = \theta^2(x_0),\ \theta[\theta^2(x_0)] = \theta^3(x_0),\ \text{and so forth,}$$
$$x_1 = \theta(x_0),\ x_2 = \theta^2(x_0) \ldots . x_{n-1} = \theta^{n-1}(x_0),\ x_0 = \theta^n(x_0). \tag{3}$$

Hence the rational function $\theta(x_0)$ has the "period" n and the *n roots "form one cycle."* Now an irreducible equation whose roots are rationally expressible in terms of one of them and form one cycle like (3) is called an *Abelian** *equation,* thus we have the result:

Every cyclic equation is an Abelian equation.

74. Let us now, conversely, determine the group G of an irreducible equation $f(x) = 0$, whose n roots satisfy the relation (3). We may unite these relations in one formula

$$x_z = \theta^z(x_0) \qquad (z = 0, 1, 2 \ldots .), \tag{4}$$

if we agree to consider two indices which are congruent (mod n) as equivalent, so that $x_z, x_{z+n}, x_{z+2n} \ldots .$ represent indifferently the same root.

Let now
$$t = \begin{pmatrix} x_0 \ldots . x_z \ldots . \\ x_a \ldots . x_{z'} \ldots . \end{pmatrix}$$

---

*Properly, *uniserial Abelian* ("einfache Abel'sche," Kronecker); no mistake can arise from this abbreviation, as I shall confine myself in this paper to the consideration of uniserial Abelian equations.

be any substitution of the unknown group G of (1); the relation (4) must then remain true if operated upon by t, hence we have

$$x_{z'} = \theta^z(x_\alpha);$$

but according to (3),

$$\theta^z(x_\alpha) = \theta^z[\theta^\alpha(x_0)] = \theta^{z+\alpha}(x_0) = x_{z+\alpha};$$

therefore $x_{z'} = x_{z+\alpha}$ and consequently

$$z' \equiv z + \alpha \qquad (\text{mod } n).$$

The substitutions of G are therefore all of the form

$$\begin{pmatrix} x_0 & x_1 & x_2 & \dots \\ x_\alpha & x_{\alpha+1} & x_{\alpha+2} & \dots \end{pmatrix},$$

or, as we may write

$$\begin{pmatrix} x_z \\ x_{z+\alpha} \end{pmatrix} \qquad (\text{mod } n), \tag{5}$$

or $|z \quad z+\alpha|$ (mod n) in Jordan's notation.

The substitution $\begin{pmatrix} x_z \\ x_{z+\alpha} \end{pmatrix}$ is the α^{th} power of the circular substitution

$$s = \begin{pmatrix} x_z \\ x_{z+1} \end{pmatrix} = (x_0, x_1, \dots x_{n-1}),$$

and therefore the group G must be either the cyclic group consisting of the n different powers of s or else one of its subgroups.

But since (1) is supposed to be irreducible, its group must be transitive, and therefore the latter case is to be excluded, since all the subgroups of the cyclic group are intransitive. Thus we find the result:

The group of an abelian equation of the n^{th} degree is a cyclic group of order n.

The terms "cyclic equation" and "abelian" equation are therefore equivalent.

75. If the degree n is prime, the cyclic group G is simple; if, on the contrary, n is composite, let p be any prime factor of n: $n = p.n'$.

If, then, we put $s^p = s'$, the group

$$H = [1, s', s'^2, \dots s'^{n'-1}]$$

is a subgroup of G of prime index p and is moreover self-conjugate under G, since $s^{-\beta}.s^{\alpha p}.s^\beta = s^{\alpha p}$ (see No. 36). In decomposing G we may therefore use H as the second group of a series of composition (No. 43). Repeating the same conclusion with the group H we find: *The factors of composition of a cyclic group of order n are the prime factors of n*, each one repeated as many times as it is contained in n.

Combining this with the results of No. 71, 4 and No. 72, we have the theorem:

An abelian equation of composite degree n can be reduced to a chain of abelian equations whose degrees are the prime factors of n.

76. *An abelian equation of prime degree is always solvable by radicals.*

Proof: Let us adjoin to our domain of rationality an imaginary n^{th} root of unity, ω, and consider the then rational function of the roots of (1):

$$V = x_0 + \omega x_1 + \omega^2 x_2 + \ldots . \omega^{n-1} x_{n-1}, \tag{6}$$

which is called *Lagrange's expression*, and is usually denoted by (ω, x_0). If operated upon by the circular substitution

$$s = (x_0, x_1, x_2, \ldots . x_{n-1}),$$

V is changed into $V_s = \omega^{-1} V$, and consequently the n^{th} power $V^n = (\omega, x_0)^n$ remains unaltered by all the substitutions of G and *a fortiori* also by all the substitutions of the group G' of (1) after the adjunction of ω (see No. 69); it is therefore (No. 62, A) rationally known:

$$V^n = \text{Rat.}\,(\omega, \mathfrak{R}', \mathfrak{R}'', \ldots .) = r(\omega). \tag{7}$$

But the function V belongs to the group 1, and therefore the roots of (1) are rationally expressible in terms of $V = \sqrt[n]{r(\omega)}$, according to Lagrange's theorem:

$$x_\alpha = \Psi_\alpha(V, \omega), \tag{8}$$
$$\alpha = 0, 1, \ldots . n-1.$$

Hence the equation (1) is, in fact, solvable by radicals, provided the n^{th} root of unity ω be known.

The expression of x_α in terms of V can be found in a very elegant way by the following method due to Lagrange: Evidently also the function $(\omega^\kappa, x_0)^n$ is rationally expressible in terms of ω, say

$$(\omega^\kappa, x_0)^n = r_\kappa(\omega).*$$

---

* It can be proved that $r_\kappa(\omega) = r(\omega_\kappa)$.

Forming this equation for $\varkappa = 1, 2, \ldots . n-1$ and extracting the n^{th} root, we obtain

$$\begin{aligned}
x_0 + \omega x_1 \quad &+ \ldots . + \omega^{n-1} x_{n-1} = \sqrt[n]{r_1(\omega)}, \\
x_0 + \omega^2 x_1 \quad &+ \ldots . + \omega^{2(n-1)} x_{n-1} = \sqrt[n]{r_2(\omega)}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
x_0 + \omega^{n-1} x_1 &+ \ldots . + \omega^{(n-1)^2} x_{n-1} = \sqrt[n]{r_{n-1}(\omega)}.
\end{aligned}$$

Combining these equations with the following:

$$x_0 + x_1 + \ldots . + x_{n-1} = c_1,$$

we have a system of n linear equations, from which we deduce, by multiplying the first by $\omega^{-\alpha}$, the second by $\omega^{-2\alpha}$, and so on, and adding,

$$x_\alpha = \frac{c_1 + \omega^{-\alpha}\sqrt[n]{r_1(\omega)} + \omega^{-2\alpha}\sqrt[n]{r_2(\omega)} \ldots . + \omega^{-(n-1)\alpha}\sqrt[n]{r_{n-1}(\omega)}}{n},$$

$$\alpha = 1, 2 \ldots . n.$$

The value of one of the $n-1$ radicals which enter into these expressions, for instance $\sqrt[n]{r_1(\omega)}$, may be chosen arbitrarily; the others are then completely determined, since they are rationally expressible in terms of the first; in fact, the quotient

$$\frac{\sqrt[n]{r_\kappa(\omega)}}{\sqrt[n]{r_1(\omega)}} = \frac{(\omega^\kappa, x_0)}{(\omega, x_0)^\kappa}$$

remains unaltered by all the substitutions of G, and is therefore rationally expressible in terms of ω.

77. To obtain the primitive n^{th} root of unity ω we have to solve the equation

$$x^{n-1} + x^{n-2} + \ldots . + x + 1 = 0, \tag{9}$$

called *the equation for the division of the circle* in n equal parts, whose roots are $\omega, \omega^2, \omega^3, \ldots . \omega^{n-1}$.

This equation is itself an *abelian* equation with respect to the domain $\mathfrak{R} = 1$, if n is prime, as we suppose it to be.

For, in this case, the equation (9) is in the first place irreducible (proofs by Gauss, Eisenstein, Kronecker and others; see Jordan, No. 413, 414; Serret, No. 110; Netto, §160).

Further, all the roots are rationally expressible in terms of one of them and can moreover be arranged in one cycle; for if g denote a primitive root of the prime number n, the roots of (9) may be written

$$x_0 = \omega, \; x_1 = \omega^g, \; x_2 = \omega^{g^2}, \ldots . \, x_{n-2} = \omega^{g^{n-2}},$$

or if we write $x_0^g = \theta(x_0)$:

$$x_1 = \theta(x_0),\ x_2 = \theta^2(x_0) \dots . x_{n-2} = \theta^{n-2}(x_0),\ x_0 = \theta^{n-1}(x_0);$$

the equation (9) is therefore (No. 74) in fact an abelian equation.

According to No. 75, it can be resolved into a chain of abelian equations whose degrees are the prime factors of $n-1$. Applying to these abelian equations the method of No. 76, it follows by an easy induction that the equation (9) and consequently (No. 76), every abelian equation of prime degree is solvable by radicals.*

§16.—*Metacyclic or Galoisian Equations.*

78. In No. 74 we have represented the circular substitution $(x_0, x_1, \dots x_{n-1})$ in the abbreviated form

$$\begin{pmatrix} x_z \\ x_{z+1} \end{pmatrix} \text{ or } |z\ z+1|.$$

Similarly any substitution

$$\begin{pmatrix} x_0 & x_1 & \dots . & x_{n-1} \\ x_\alpha & x_\beta & \dots . & x_\lambda \end{pmatrix}$$

$(\alpha, \beta, \dots . \lambda$ being some permutation of the numbers $0, 1, \dots . n-1)$ may be represented in the form

$$\begin{pmatrix} x_z \\ x_{\phi(z)} \end{pmatrix} \text{ or } |z\ \phi(z)|, \tag{1}$$

if $\phi(z)$ be a function of the index z which takes for $z = 0, 1 \dots . n-1$ the values $\alpha, \beta, \dots . \lambda$ respectively. It is easy to construct such a function, for instance by means of Lagrange's Interpolation-Formula.

If, in particular, n is a prime number, $n = p$, and we agree again to consider two indices which are congruent (mod p) as equivalent, then it is always possible to choose for $\phi(z)$ an integral function with integral coefficients; and conversely,

---

*References concerning *uniserial Abelian* equations: Abel, Œuvres I; Jordan, No. 400, 401; Serret, No. 532, 533; Netto, §172. Further: Kronecker, Berliner Monatsberichte, 1853; Weber, Theorie der Abel'schen Zahlkörper, Acta Math., Vol. 8, 9.

Concerning the equation for the *division of the circle* in particular, see Bachman, Die Lehre von der Kreisteilung.

Concerning the most general kind of Abelian equations, so-called *manyfold* ("mehrfaltige," Kronecker) Abelian equations, see Abel, Œuvres I; Jordan, No. 402–415; Netto, §160–187; Serret, No. 529–554, and Kronecker, Berliner Monatsberichte, 1870.

any such function will be apt to represent a substitution between p letters if the p values which it takes for $z = 0, 1, \dots p - 1$ form a complete system of remainders (mod n). Hermite has given, in this respect, the following criterion, necessary and sufficient:

Form the first $p - 2$ *powers of* $\phi(z)$:

$$\phi(z),\ [\phi(z)]^2, \dots [\phi(z)]^{p-2},$$

and reduce them to the degree $p - 1$ *by means of Fermat's theorem*:

$$z^p \equiv z \pmod{p},$$

then the coefficient of z^{p-1} *in every one of these reduced functions must be divisible by* p (see Serret, No. 474–476; Jordan, No. 114, 115; Netto, §§134, 135).

Remark: Since the order in which the letters in the first line of a given substitution are written may be chosen arbitrarily (No. 3), we may represent the substitution

$$\binom{x_z}{x_{\phi(z)}} \text{ also by the symbol } \binom{x_{\psi(z)}}{x_{\phi[\psi(z)]}},$$

$\psi(z)$ denoting a function satisfying Hermite's criterion ("Transformation of the index").

79. This "analytical representation" of a substitution is useful in solving the problem: *To determine the largest substitution-group between the letters* $x_0, x_1, \dots x_{p-1}$ *of which the cyclic group*

$$H = \binom{x_z}{x_{z+c}} \pmod{p}, \quad c = 0, 1, \dots p - 1$$

is a self-conjugate subgroup.

Let

$$g = \binom{x_z}{x_{\phi(z)}}$$

be any substitution of the sought group G; then the transformed of the substitution

$$h = \binom{x_z}{x_{z+1}}$$

by g must again belong to the self-conjugate subgroup H (No. 36), and consequently be some power of h, say

$$g^{-1}hg = h^a.$$

Now we have (compare the remark in No. 78),

$$g^{-1} = \begin{pmatrix} x_{\phi(z)} \\ x_z \end{pmatrix}, \quad g^{-1}h = \begin{pmatrix} x_{\phi(z)} \\ x_{z+1} \end{pmatrix}, \quad g^{-1}hg = \begin{pmatrix} x_{\phi(z)} \\ x_{\phi(z+1)} \end{pmatrix};$$

on the other hand, we may write

$$h^a = \begin{pmatrix} x_{\phi(z)} \\ x_{\phi(z)+a} \end{pmatrix}.$$

Consequently $\psi(z)$ must satisfy the condition

$$\phi(z+1) \equiv \phi(z) + a \qquad (\mathrm{mod}\ p),$$

for $z = 0, 1, 2, \ldots . Z \ldots . p-1$; that is,

$$\left.\begin{array}{lll} \phi(1) \equiv \phi(0) + a & & \\ \phi(2) \equiv \phi(1) + a & \equiv \phi(0) + 2a, & \\ \ldots\ldots\ldots\ldots\ldots\ldots & & \\ \phi(Z) \equiv \phi(Z-1) + a & \equiv \phi(0) + Za, & \end{array}\right\} (\mathrm{mod}\ p),$$

or if we put $\phi(0) = b$ and write z instead of Z,

$$\phi(z) \equiv az + b \quad (\mathrm{mod}\ p).$$

Therefore all the substitutions of the sought group G must be of the form

$$\begin{pmatrix} x_z \\ x_{az+b} \end{pmatrix}.$$

Conversely, it is easily seen that this symbol always represents a substitution, provided a be not divisible by p. There are on the whole $p(p-1)$ *different* substitutions of this form, corresponding to the values

$$a \equiv 1, 2, \ldots . p-1; \ b \equiv 0, 1, \ldots . p-1 \qquad (\mathrm{mod}\ p).$$

These $p(p-1)$ substitutions form a group called the *metacyclic group;* this is then the largest group between the letters $x_0, x_1, \ldots . x_{p-1}$ that contains the given cyclic group as a self-conjugate subgroup.

Besides the powers of the substitution $\begin{pmatrix} x_z \\ x_{z+1} \end{pmatrix}$, the metacyclic group contains no other circular substitution of the order p. For the substitution

$$\begin{pmatrix} x_z \\ x_{az+b} \end{pmatrix}$$

leaves, if a is not congruent 1 (mod p), one root unaltered, viz. that one whose index is determined by the congruence

$$az + b \equiv z \pmod{p}.$$

80. An equation of the p^{th} degree,

$$f(x) = 0, \tag{1}$$

whose group G is the metacyclic group, is called a *metacyclic equation.* It has the following two characteristic properties:

a). It is *irreducible,* for the metacyclic group is evidently transitive (No. 65).

b). *All its roots are rationally expressible in terms of two of them.*

For it is easily seen that the substitution 1 is the only substitution of the metacyclic group which leaves at the same time the two roots x_0 and x_1 unaltered. Hence the function $V = m_0x_1 + m_1x_1$ "belongs" (No. 67) to the group 1, and therefore all the roots are rationally expressible in terms of V, or what amounts to the same, in terms of x_0 and x_1:

$$x_2 = \theta_2(x_0, x_1); \ldots . x_{p-1} = \theta_{p-1}(x_0, x_1). \tag{2}$$

Now an *irreducible* equation of *prime degree, whose roots are rationally expressible in terms of two of them,* is called a *Galoisian equation.* Thus we have the result:

A metacyclic equation is always a Galoisian equation.

81. Let us now, conversely, determine the group of a Galoisian equation of the p^{th} degree.

a). Since the equation is supposed to be irreducible, its group G must be *transitive,* and therefore its *order divisible by the degree p* (No. 24).

b). Since, moreover, p is supposed to be prime, G *must contain a cyclic subgroup H, of order p,* according to Cauchy's theorem (No. 22); we may suppose that it consists of the different powers of the circular substitution

$$a = (x_0, x_1, \ldots . x_{p-1}),$$

x_0 and x_1 denoting the two roots in terms of which all the others are supposed to be expressible rationally.*

c). This cyclic subgroup H must be *self-conjugate* under G. In fact, if it were otherwise, G would contain two circular substitutions of the order p which are not powers of one another (No. 36), but this is impossible.

---

*For among the different powers of any circular substitution of the order p there is always one which replaces x_0 by x_1.

For let $b = (x_{i_0}, x_{i_1}, \dots . x_{i_{p-1}})$ be another circular substitution* of the order p contained in G. It is then always possible to choose two integers, μ and ν, *incongruent* (mod p), such that

$$i_{\mu+1} - i_\mu \equiv i_{\nu+1} - i_\nu, \text{ say } \equiv k \pmod{p}.$$

Applying, then, according to No. 62, B′, the two substitutions $b^\mu a^{-i_\mu}$ and $b^\nu a^{-i_\nu}$ of G to the rational relations

$$x_{i_\alpha} = \theta_\alpha(x_{i_0}, x_{i_1}),$$
$$(\alpha = 0, 1, \dots . p-1)$$

we obtain

$$x_{i_{\alpha+\mu}-i_\mu} = \theta_\alpha(x_0, x_\kappa),$$
$$x_{i_{\alpha+\nu}-i_\nu} = \theta_\alpha(x_0, x_\kappa),$$

and consequently

$$i_{\alpha+\mu} - i_\mu = i_{\alpha+\nu} - i_\nu \qquad (\alpha = 0, 1, \dots . p-1).$$

Hence follows† that the p differences $i_{\beta+1} - i_\beta$ $(\beta = 0, 1, \dots . p-1)$ have the same value, say m; that is to say, $b = a^m$. Q. E. D.

d). Since the cyclic group H is a self-conjugate subgroup of G, G must be the metacyclic group or one of its transitive subgroups (No. 79), thus we have the result:

The group of a Galoisian equation is the metacyclic group or one of its transitive subgroups.

82. In order to solve a metacyclic equation we construct (No. 58) a rational function ψ of the roots which belongs to the cyclic subgroup H; ψ satisfies, then, (No. 67) a resolvent equation of the degree $p-1$: $g(\psi) = 0$. To determine its group Γ (No. 71) we remark that the metacyclic group may be generated by the two substitutions

$$a = \begin{pmatrix} x_z \\ x_{z+1} \end{pmatrix} \text{ and } c = \begin{pmatrix} x_z \\ x_{gz} \end{pmatrix},$$

g denoting a primitive root of the prime number p. The substitutions of the metacyclic group are then $a^\alpha c^\gamma$ $(\alpha = 0, 1, \dots . p-1;\ \gamma = 1, 2, \dots . p-1)$, and

---

[*] We may suppose $i_0 = 0$, $i_1 = 1$ by replacing, eventually, b by a convenient power of b.

[†] See Kronecker, Berliner Monatsberichte, 1879.

those of the cyclic subgroup H are a^α $(\alpha = 0, 1, \ldots . p-1)$. Hence the $p-1$ conjugate values of ψ under G are (No. 23)

$$\psi_0 = \psi, \ \psi_1 = \psi_c, \ \psi_2 = \psi_{c^2}, \ldots . \psi_{p-2} = \psi_{c^{p-2}}.$$

The cyclic group H being self-conjugate under G, the ψ's undergo the substitution $(\psi_0, \psi_1, \ldots . \psi_{p-2})^\beta$, when the x's are operated upon by the substitution $a^\alpha b^\beta$, and therefore (No. 71) the group Γ of the resolvent equation $g(\psi) = 0$ is the cyclic group of order $p-1$, consisting of the different powers of the substitution $(\psi_0, \psi_1, \ldots \psi_{p-2})$, and consequently the resolvent is an Abelian equation.

By the adjunction of ψ the group of the equation $f(x) = 0$ is reduced to the cyclic subgroup H (No. 70); the equation $f(x) = 0$ is therefore an Abelian equation in the new domain of rationality.

Analogous results are obtained for the transitive subgroups of the metacyclic group, which are all contained in the form

$$a^\alpha c^{\delta\gamma},$$
$$\left(\alpha = 0, 1, \ldots . p-1; \ \gamma = 1, 2, \ldots . \frac{p-1}{\delta}\right),$$

δ denoting any divisor of $p-1$. Thus we find the result:

A Galoisian equation can always be solved by a chain of two Abelian equations, the first of degree $p-1$ $\left(\text{resp.} \frac{p-1}{\delta}\right)$, *the second of degree* p, and consequently (No. 75):

A Galoisian equation is always solvable by a chain of Abelian equations of prime degree; and finally (No. 76):

A Galoisian equation is always solvable by radicals.

83. An important example of Galoisian equations are the *binomial equations of prime degree:*

$$x^p = A,$$

where A is supposed to be a rational quantity which is not expressible as a p^{th} power of another rational quantity.

For, in the first place, the binomial equation is *irreducible* under these circumstances, as Abel has proved (see Jordan, No. 418; Netto, §203).

Further, if x_0 be one of its roots and ω an imaginary p^{th} root of unity, the other roots are

$$x_1 = \omega x_0, \ x_2 = \omega^2 x_0, \ \ldots . \ x_{p-1} = \omega^{p-1} x_0,$$

hence $\omega = \frac{x_1}{x_0}$ and consequently

$$x_a = \left(\frac{x_1}{x_0}\right)^a x_0 \qquad (a = 0, 1, \ldots . p - 1).$$

All the roots are therefore rationally expressible in terms of two of them. The equation is therefore indeed a Galoisian equation.

For the function ψ of No. 82 which belongs to the cyclic subgroup, we may choose, in this case, the quantity ω, since

$$\omega = \frac{x_1}{x_0} = \frac{x_2}{x_1} = \ldots . = \frac{x_0}{x_{p-1}} .$$

ω satisfies the resolvent equation of the degree $p - 1$:

$$\omega^{p-1} + \omega^{p-2} + \ldots . + \omega + 1 = 0,$$

which is, in fact, an Abelian* equation (No. 77).

After the adjunction of ω the binomial equation is itself an Abelian, the function $\theta(x_0)$ being in this case $\theta(x_0) = \omega x_0$ (compare also No. 64).

Hence follows that *a binomial equation of prime degree is always solvable by a chain of Abelian equations of prime degree.*†

§17.—*Solution by Radicals.*

84. The equation of the n^{th} degree

$$f(x) = 0 \tag{1}$$

is said to be *solvable by radicals* if its roots can be derived from the known quantities $\mathfrak{R}', \mathfrak{R}'', \ldots .$ by a finite number of extractions of roots whose exponents may, without loss of generality, be supposed to be prime. If $\xi, \eta, \ldots . \psi$ denote all the radicals which occur in the expressions for all the roots $x_1, x_2, \ldots . x_n$, the solution may be written in the form of a chain of binomial equations of prime degree:

---

*For certain special domains of rationality it may, however, happen that ω satisfies an Abelian of degree $\frac{p-1}{\delta}$.

† This holds still if the binomial equation is reducible; for, in this case, one root is rational (Netto, §203), and the problem is reduced to the determination of ω.

References concerning Galoisian equations: Jordan, No. 416–418; Netto, §187–190; Kronecker, Berliner Monatsberichte, 1879.

$$\left.\begin{array}{l}
\xi^{\lambda} = L(\mathfrak{R}', \mathfrak{R}'', \ldots .), \\
\eta^{\mu} = M(\xi;\ \mathfrak{R}', \mathfrak{R}'', \ldots .), \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\psi^{\rho} = P(\phi, \ldots . \eta, \xi;\ \mathfrak{R}', \mathfrak{R}'', \ldots .), \\
x_{\alpha} = R_{\alpha}(\psi, \phi, \ldots . \eta, \xi;\ \mathfrak{R}', \mathfrak{R}'', \ldots .),
\end{array}\right\} \qquad (2)$$

$$\alpha = 1,\ 2, \ldots .\ n,$$

$L, M, \ldots . P, R_{\alpha}$ denoting rational functions with integral coefficients,* and the degrees $\lambda, \mu, \ldots . \rho$ being prime numbers.

Now, according to No. 83, every one of these binomial equations, and consequently also the whole chain, can be replaced by a chain of Abelian equations of prime degrees, and since conversely every Abelian equation is solvable by radicals, we have the result:

In order that an equation be solvable by radicals, it is necessary and sufficient that it be reducible to a chain of Abelian equations of prime degrees:

$$\left.\begin{array}{l}
\Phi(y;\ \mathfrak{R}', \mathfrak{R}'', \ldots .) = 0, \\
\Psi(z;\ y, \mathfrak{R}', \mathfrak{R}'', \ldots .) = 0, \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\Lambda(w;\ v, \ldots . z, y, \mathfrak{R}', \mathfrak{R}'', \ldots .) = 0, \\
x_{\alpha} = R_{\alpha}(w, v, \ldots . y, \mathfrak{R}', \mathfrak{R}'', \ldots .),
\end{array}\right\} \qquad (3)$$

$$\alpha = 1,\ 2, \ldots .\ n.$$

The first of these equations is an Abelian equation with respect to the domain $(\mathfrak{R}', \mathfrak{R}'', \ldots .)$, the second with respect to the enlarged domain $(y, \mathfrak{R}', \mathfrak{R}'', \ldots .)$ and so forth.

Since the group of a binomial equation is more complicated than that of an Abelian (No. 83), we have, from our present point of view, to consider as the simplest possible class of equations not the binomial, but the Abelian equations of prime degree, and therefore it is preferable to start, in our developments, from the chain of Abelian equations (3).

85. Let now G denote the group of the equation (1)—which we suppose to be solvable by the chain (3)—with respect to the original domain of rationality $(\mathfrak{R}', \mathfrak{R}'', \ldots .)$.

We begin the solution by solving the first equation of the chain (3) and adjoining one of its roots, y, to our domain; the group G of (1) is then reduced to a certain subgroup (No. 69), say H (including the case $H = G$). Next we solve the second equation and adjoin one of its roots, z, to our present domain; the group H of (1) is then reduced to a subgroup, say I (including again the case $I = H$). Continuing in this way, we arrive at last, after solving the last equation, at the domain

---

* It is always to be understood that some of the quantities $\xi, \eta, \ldots . \psi$ may be wanting in the expression of R_{α}, and similarly for the other functions.

$$(w, v, \ldots . z, y, \mathfrak{R}', \mathfrak{R}'', \ldots .);$$

with respect to this domain, the group of (1) *is* 1, since all the roots are rationally known with respect to it (No. 63, a).

Now I say: By every one of these successive adjunctions the group of (1) is either not reduced at all or it is reduced to a *self-conjugate* subgroup of *prime index.*

Proof: I). Let ν be the index of the subgroup H, to which the group G of (1) is reduced after the adjunction of the root $y_1 = y$ of the first Abelian equation

$$\Phi(y; \mathfrak{R}', \mathfrak{R}'', \ldots .) = 0, \tag{4}$$

whose degree, p, is supposed to be prime.

a). Let, moreover, $\phi(x_1, x_2, \ldots . x_n)$ denote a rational function of the roots which belongs to the group H (No. 67 and 58); ϕ will then satisfy a resolvent equation

$$g(\phi) = 0, \tag{5}$$

of degree ν and irreducible in the domain $(\mathfrak{R}', \mathfrak{R}'', \ldots .)$ (No. 71).

b). On the other hand, H being the group of (1) in the enlarged domain

$$(y_1, \mathfrak{R}', \mathfrak{R}'', \ldots .),$$

ϕ is rationally expressible in terms of y_1 (No. 62, A):

$$\phi = r(y_1). \tag{6}$$

Applying now the theorem of No. 71, 5 to the rational function $\phi = r(y_1)$ of the root y_1 of the irreducible (since Abelian) equation (4), we obtain a second resolvent equation for ϕ:

$$h(\phi) = 0, \tag{7}$$

likewise irreducible and whose degree is a divisor of the degree p of (6) and consequently either $= 1$ or $= p$, since p is prime.

c). But the two equations (5) and (7), being both irreducible and having the root ϕ in common, must be identical (No. 57), and therefore the degree ν of (5), that is to say, the index of H under G, must be either $= 1$ or $= p$. Thus we find: *By the adjunction of a root* $y_1 = y$ *of an irreducible equation of prime degree* p, *the group of* (1) *is either not reduced at all or it is reduced to a subgroup of index* p.

II. In the latter case the p roots of (7), which are

$$r(y_1),\ r(y_2),\ \ldots\ r(y_p),$$

$y_1, y_2, \ldots y_p$ denoting the p roots of (4), must be identical with the roots of (5), which are the $\nu = p$ conjugate values $\phi_1 = \phi$, $\phi_2 \ldots \phi_p$ of ϕ under G, derived from ϕ by certain substitutions $g_1 = 1$, $g_2, \ldots g_p$ of G. We may therefore write

$$\phi_\alpha = r(y_\alpha), \qquad (8)$$
$$\alpha = 1, 2, \ldots p.$$

Now the function ϕ_α of the roots of (1) belongs to the subgroup $g_\alpha^{-1}Hg_\alpha$ of G (No. 35), and any rational function of the roots which remains unaltered by the same group $g_\alpha^{-1}Hg_\alpha$ is rationally expressible in terms of ϕ_α (No. 67) and consequently also in terms of y_α.

If, therefore, instead of the root $y_1 = y$ of (4), we adjoin the root y_α, the group G' of (1) with respect to the domain $(y_\alpha, \mathfrak{R}', \mathfrak{R}'', \ldots)$ must be either $g_\alpha^{-1}Hg_\alpha$ or one of its subgroups (No. 63, a); but the latter case is impossible; for, according to No. 85, the index of G' under G must be either 1 or p, and the index of $g_\alpha^{-1}Hg_\alpha$ under G is p, hence $G' = g_\alpha^{-1}Hg_\alpha$. Thus we find:

If, instead of the root y_1, *we adjoin another root* y_α *of* (4), *the group* G *is reduced to a subgroup* $H_\alpha = g_\alpha^{-1}Hg_\alpha$ CONJUGATE WITH H UNDER G.

III. If now, in particular, the auxiliary equation (4) is an *Abelian* equation, as we suppose, then y_α is rationally expressible in terms of y_1:

$$y_\alpha = \theta(y_1);$$

but also, conversely, y_1 is rationally expressible in terms of y_α; for, according to No. 73, we have

$$\theta^p(y_1) = y_1,$$

therefore

$$\theta^{p-1}(y_\alpha) = \theta^p(y_1) = y_1.$$

Hence the two domains of rationality $(y_1, \mathfrak{R}', \mathfrak{R}'', \ldots)$ and $(y_\alpha, \mathfrak{R}', \mathfrak{R}'', \ldots)$ are identical and the group of (1) must be the same with respect to either of them. Therefore $g_\alpha^{-1}Hg_\alpha = H$, for $\alpha = 1, 2, \ldots p$, consequently (No. 36) H is a self-conjugate subgroup of G. Thus we have the result:

By the adjunction of a root of an Abelian equation of prime degree p, *the group* *of the given equation is either not reduced at all, or it is reduced to a self-conjugate subgroup of index* p.

Remark: To appreciate fully the importance of this theorem, which is due to Galois, we must bear in mind that *the adjoined quantity* y *is not supposed to be a rational function of the roots* $x_1, x_2, \ldots . x_n$; hence this theorem comprises, as will be seen presently, Abel's celebrated theorem that the radicals which enter into the solution of a solvable equation are always rationally expressible in terms of the roots and of certain roots of unity.

86. Applying this theorem to every one of the successive Abelian equations of the chain (3), we find that the different groups through which we pass in the process of successive adjunction must form a series of groups beginning with G, ending with 1, and such that each group is a self-conjugate subgroup of prime index of the group immediately preceding, or, according to No. 43: The factors of composition of the group G must all be prime numbers.

But this condition is also sufficient. For if $\lambda, \mu, \ldots . \rho$ denote the factors of composition of the group G, then we can, according to No. 72, solve the given equation by a chain of simple regular equations of the degrees $\lambda, \mu, \ldots . \rho$; and if, in particular, the factors of composition are all prime numbers, then these regular equations are Abelian equations of prime degrees (No. 71, 4), and therefore the given equation is solvable by radicals.

Thus we have proved Galois' criterion for the solution by radicals: *In order that an equation be solvable by radicals, it is necessary and sufficient that the factors of composition of its group be all prime numbers.*

Remark: At the same time we see from No. 72 that we may choose, for the auxiliary quantities $y, z, \ldots . v, w$ of the chain (3), *rational functions of the roots* $x_1, x_2, \ldots . x_n$. If, then, we transform the chain of Abelian equations into a chain of binomial equations, by means of the theorem of No. 76, we obtain Abel's theorem mentioned in the remark in No. 85.*

87. The group of the general equation of the n^{th} degree is the symmetric group (No. 66), whose factors of composition are for $n > 4$ (No. 44): 2 and $\frac{n!}{2}$; the latter being composite, *the general equation of a higher than the fourth degree is not solvable by radicals.*

---

* Since the above was written, an important paper on the solution of equations by means of a chain of auxiliary equations has been published by Hölder: Zurückführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen (Math. Annalen, Bd. 34).

For $n = 3$ the factors are 2, 3; for $n = 4$ they are 2, 3, 2, 2 (No. 43), all of them prime; this is the reason why the general equations of the third and fourth degree are solvable by radicals.

Their solution by a chain of Abelian equations is exhibited in the following tables:

a). *Cubic equation* (Notations of No. 14):

$$x^3 - c_1x^2 + c_2x - c_3 = 0. \tag{1}$$

Domain of rationality.	Group of (1)
Original domain: (c_1, c_2, c_3): $\phi = (x_2 - x_3)(x_3 - x_1)(x_1 - x_2)$ belongs to G_3; $\phi^2 - \Delta = 0$, Abelian.	G_6
Adjoin ϕ: x_1 belongs to $G_1 = 1$; and (1) itself is Abelian.	G_3
Adjoin x_1: The other roots are now rationally known; their expressions are given in Serret, No. 511.	1

b). *Biquadratic equation*, Ferrari's solution (Notations of No. 15–18):

$$x^4 - c_1x^3 + c_2x^2 - c_3x + c_4 = 0. \tag{1}$$

Domain of rationality.	Group of (1)
Original domain (c_1, c_2, c_3, c_4): $\phi = \Pi(x_\alpha - x_\beta)$ belongs to G_{12}; $\phi^2 - \Delta = 0$, Abelian.	G_{24}
Adjoin ϕ: $\xi_1 = x_1x_2 + x_3x_4$ belongs to G_4, $\xi^3 - c_2\xi^2 + (c_1c_3 - 4c_4)\xi - [c_4(c_1^2 - 4c_2) + c_3^2] = 0$, Abelian.	G_{12}

Adjoin ξ_1: $\eta = x_1 + x_2 - x_3 - x_4$ belongs to G_2, $\eta^2 - 4\xi_1 - c_1^2 + 4c_2 = 0$, Abelian.	G_4
Adjoin η: x_1 belongs to $G_1 = 1$, $x^2 - \left(\frac{c_1 + \eta}{2}\right)x + \left(\frac{\xi_1}{2} + \frac{c_1\xi_1 - 2c_3}{2\eta}\right) = 0$, Abelian.	G_2
Adjoin x_1: The other roots are now rationally known; this is evident for x_2; to find the expressions for x_3 and x_4, notice that $\xi_2 - \xi_3 = (x_1 - x_2)(x_3 - x_4)$ is rationally expressible in terms of ξ_1 and $\sqrt{\Delta}$ (see Serret, No. 511, equation (3)).	1

88. Let us now determine all *irreducible* equations of *prime degree* which are *solvable by radicals.*

Let
$$f(x) = 0 \tag{1}$$
be the given equation of prime degree p, G its group and
$$G - H - \ldots . K - L \ldots . 1, \tag{2}$$
a series of composition of G.

The factors of composition are then all prime numbers since (1) is supposed to be solvable by radicals (No. 86).

I). The group G must be transitive, since (1) is supposed to be irreducible (No. 65), and therefore its order must be divisible by p (No. 24); since, moreover, p is supposed to be prime, *G must contain a circular substitution of order p* (No. 22), say
$$t = \binom{x_z}{x_{z+1}} \quad (\text{mod } p).$$

In the series (2) there must necessarily exist one group, K, such that this substitution t is contained in K and in all preceding groups, but is not contained in the group L immediately following K.

I say, *this group L must be the group* 1.

Proof: a). Let ν be the index of L under K; ν being prime, we may apply to the substitution t the lemma of No. 40: "If k be any substitution of K which is not contained in L, then k^ν, and no lower power of k, belongs to K; moreover, the order of the substitution k is a multiple of ν."

Now evidently $t^p = 1$ is the lowest power of t which belongs to L, therefore $\nu = p$.

b). Suppose, now, L contains a substitution s different from 1, which replaces the letter x_α by a different letter x_β. The substitution $u = st^{\alpha-\beta}$ will then leave the letter x_α unaltered.

Now u belongs to the group K, but not to L, since $\alpha - \beta$ is not divisible by p according to our assumptions; therefore, according to the lemma of No. 40, the order of u must be divisible by p, but this is impossible since u is a substitution between p letters, which leaves the letter x_α unaltered.

Consequently L can contain no substitution besides 1: $L = 1$.

II. Let us now build up the series of composition, starting from the last group $L = 1$.

a). The index of L under K is p according to I, a; therefore K *must be the cyclic group* of order p consisting of the different powers of the circular substitution t, since K is supposed to contain t.

b). Hence the group immediately preceding K in the series (2), say J, must be contained in the metacyclic group, since it contains the cyclic group of order p, viz. K, as a self-conjugate subgroup (No. 79). According to the remark at the end of No. 79, J contains then no circular substitution of order p except the powers of the substitution t.

c). Let now I be the group immediately preceding J in the series (2); J being a self-conjugate subgroup of I, the transformed of t by any substitution of I, which is again a circular substitution of order p, must belong to J (No. 36) and must therefore be some power of t, according to *b*). Hence follows that the cyclic group K must be self-conjugate not only under J but also under I, and therefore I must be contained in the metacyclic group.

d). The same conclusion holds for the group immediately preceding I, and so forth, and finally for the group G itself: G must be the metacyclic group or one of its transitive subgroups.

According to No. 81, we have therefore the theorem, due to Galois:

Every irreducible equation of prime degree which is solvable by radicals is a Galoisian equation.

The conversion has been proved previously in No. 82.*

---

* References concerning §17: Serret, No. 580 and No. 587–598; Jordan, No. 373–378, 520; Kronecker, Berliner Monatsberichte, 1879.

Concerning solvable equations whose degree is not prime, see Jordan, Livre IV; besides Journal de Mathématiques, Ser. 2, Vol. 12, 13, 14, Netto, §§233–243.

As to applications of Galois' theory to the *division of trigonometric, the division and transformation of elliptic and Abelian functions*, see Jordan, Chap. IV; Weber, Zur Theorie der elliptischen Functionen, Acta Math., Vol. 6; Kronecker, Entwicklungen aus der Theorie der Gleichungen, Berliner Monatsb. 1879.

As to applications to geometrical problems, see Jordan, Chap. III.

CONTENTS.

PART I. Theory of substitution-groups, ... 59
§1. Introduction: Lagrange's Researches, ... 60
§2. Elementary propositions on substitutions, ... 65
§3. Rational functions and substitution-groups, ... 71
§4. Group and subgroup, ... 78
§5. Algebraic relations between different rational functions, ... 81
§6. Chains of resolvent equations, ... 84
§7. Conjugate groups, ... 88
§8. Group between the conjugate values of a function, ... 92
§9. Decomposition of a group, ... 97
§10. Groups of operations, ... 102

PART II. Galois' theory of algebraic equations, ... 109
§11. Galois' resolvent, ... 109
§12. Group of an equation, ... 113
§13. Theorems on asymmetric functions of the roots, ... 118
§14. Reduction of the group by adjunction, ... 121
§15. Cyclic or Abelian equations, ... 124
§16. Metacyclic or Galoisian equations, ... 128
§17. Solution by radicals, ... 134

EXPLANATION OF SOME TERMS.

Adjunction of a quantity, No. 69.
Belongs, a function—to a group No. 13, 67.
Conjugate values of a function, No. 23; substitutions, No. 35; subgroups, No. 35.
Cyclic group, No. 20; equation, No. 73.
Discriminant of a function, No. 28.
Domain of rationality, No. 56.
Even substitutions, No. 16.
Four-group, No. 17.
Group of a rational function, No. 13.
Index of a subgroup, No. 22.
Interchangeable substitutions, No. 11.
Maximum self-conjugate subgroup, No. 43.
Metacyclic group, No. 79; equation, 80.
Monodromy-group, No. 64.
Multiplication-table, No. 14.
Multipliers, No. 22.
Odd substitutions, No. 16.
Period of an operation, No. 12.
Rational quantity, No. 56.
Rationally known, No. 56.
Regular group, No. 24; equation, No. 68.
Self-conjugate subgroup, No. 36.
Unaltered, a function remains unaltered by a substitution, No. 7, 56.*

BALTIMORE, MD., *May* 1889.

---

* To the text-books enumerated at the beginning of this paper may be added *Chrystal's Algebra*, whose second volume (published since the above was written) contains a chapter on the theory of substitutions.